S E M I N A R E

Microsoft

2224

Cyber Security - Ethical Hacking und Forensic Basic (MS IT Boot-Camp)

o Zielgruppe

Dieser Kurs richtet sich an IT-Fachleute, die Kenntnisse zur Cyber Security erwerben möchten.

o Voraussetzungen

Praktische Erfahrungen in der Administration von Windows-Infrastrukturen.

o Seminarziel

Verstehe deinen Feind um dich zu schützen. Sie suchen nach einer Möglichkeit, Hackerangriffe zu verstehen und Schwachstellen in Ihrem System zu finden? Mit unserem 5-tägigen Praxisworkshop können wir Ihnen dabei helfen, genau diese Anforderung zu erfüllen.

Über 75 % des Seminars/Workshops ist Lab basiert. Wir leiten Sie in diesen Demos/Übungen an und versuchen ein Verständnis für die Möglichkeiten des White-Hat-Hacking zu vermitteln.

In diesem Workshop nehmen wir Sie mit auf die Reise in die Welt des Hackings von Windows-basierten Systemen. Dabei werden wir Rechtliches betrachten, eine Laborumgebung mit einzelnen wichtigen Werkzeugen einrichten.

Vortrag (max. 10%), Demonstration (geplant 15%) und Übungen am System (ca. 75 %)

o Seminarinhalt

Einführung Ethical Hacking
- Rechtliches
- Einführung in das Hacking
- Vorgehensweise von Hackern
- Laborumgebung einrichten (Kali, Nmap, Wireshark ....)

Informationsbeschaffung
- Informationsbeschaffung mit öffentlich zugänglichen Mitteln
- Google Hacking (Google Dorks)
- Port Scanning
- Vulnerability Scanning (Suche nach Schwachstellen)

Exploits
- Verständnis für Exploits
- Exploit Frameworks (Penetration)
- Nutzung von Exploits zur Kompromittierung von Windows-Systemen
- Exploit Frameworks am Beispiel von Metasploit

Malicious Code
- Viren und Trojaner
- Rootkits

Hacking Hardware
- Rubber Ducky & Co.
- WLAN Jammer

Windows-Schwachstellen
- Windows-Architektur und -Design, Gruppenrichtlinien
- Enumeration von Benutzern und Diensten unter Windows
- NetBIOS-spezifische Schwachstellen (Exploits, IPC, Admin Shares)
- Auslesen von Zugangsdaten (LSA Cache, Mimikatz, Lateral Movement)
- Gezielte Ausnutzung von fehlkonfigurierten Diensten und Anwendungen
- AD-/RDP-/SQL-spezifische Schwachstellen
- Fehler im Server-Handling

Microsoft

2224

Netzwerkangriffe
- Angriffe gegen Netzwerkkomponenten
- Sniffing und Passwörter abhören
- Password Cracking
- Man-in-the-Middle-Angriffe

Denial-of-Service Angriffe
- DoS und DDoS
- Amplification Attacks

Wireless LAN Hacking
- WLAN-Sicherheit
- WEP Cracking
- WPA Cracking

Verwendete Werkzeuge
- Kali Linux
- Python
- Cain & Abel
- Nmap
- Wireshark
- Nessus usw.

o Seminardauer: 5 Tage

Lernen im Schulungshotel Gröbern am See in Muldestausee/Gröbern, in der Dübener Heide.
Seminardauer: Erster Tag ab 10:00 Uhr, letzter Tag ca. 15:00 Uhr
Kleine Gruppen mit 2-4 Teilnehmer (max. 6)
Im Preis enthalten sind:
- Übernachtungskosten im Hotel
- Vollverpflegung inkl. Getränke
- Schulungsunterlagen
- täglich open end
- intensive Übungs- und Nachbereitungsphasen nach Seminarende

o Preis pro Person: 2.990 EUR netto